REMARKS

Claims 1-38 and 41-61 are pending in the application, and claims 1-5, 9-34, 36-38 and 41-61 stand rejected.

Objections to the claims

Claims 1 and 3-9 stand objected to for the spelling of the word "authorised." This is the British English spelling of the word "authorized." Applicants wish to bring the Examiner's attention to section 608.01 of the Manual of Patent Examining Procedures, which clearly directs that "Examiners should not object to the specification and/or claims in patent applications merely because applicants are using British English spellings (e.g., colour) rather than American English spellings. It is not necessary to replace the British English spellings with the equivalent American English spellings in the U.S. patent applications. Note that 37 CFR 1.52(b)(1)(ii) only requires the application to be in the English language. There is no additional requirement that the English must be American English." [emphasis in the original] Applicants thus respectfully request the Examiner to withdraw this objection.

Rejection under 35 U.S.C §112

Claims 20, 21, 27 and 35 stand rejected under 35 U.S.C. 112 as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. In particular, the Examiner finds that claim 20 is inconsistent with FIG. 1 because it recites that the "interface means is resident...within said monitoring component" and FIG. 1 "depicts that the card reader 12 is a separate component of the system 10 that also includes the monitoring component 24." Applicants have amended the specification to provide support for this claim. Support for this amendment in the originally filed application is provided by claim 20 as originally filed.

Claim 21 stands rejected for being inconsistent with FIGS. 1 and 2. This claim has been corrected to address this incongruity.

Claims 27 stand rejected for lacking antecedent basis for "said certified reference data." This claim has been amended to depend from claim 26, which provides the necessary antecedent basis.

Applicants submit that these claims are now allowable and respectfully request the Examiner to withdraw these rejections.

Rejection under 35 U.S.C §103

Claims 1, 2, 10-32, 38 and 41-61 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Pat. No. 5,923,759 to Lee in view of U.S. Pat. No. 5,822,431 to Sprunk. In particular, with regards to claim 1, the Examiner finds that Lee discloses all claimed limitations except for a monitoring component that is configured to perform a plurality of data checks on the computing platform, and that Sprunk discloses precisely this limitation. The Examiner further opines that the skilled person would have found obvious to modify Lee as taught by Sprunk because doing so "ensures that the network meets a minimum reliability standard." Applicants respectfully disagree with the Examiner's conclusion because there is no network mentioned anywhere in Lee, and thus the skilled person perusing Lee would have no motivation whatsoever to look at a reference directed to network reliability such as Sprunk. Applicants thus respectfully traverse the Examiner's holding that combining these two references would have been obvious to the skilled person, and further disagree that such a combination anticipates the instantly claimed invention.

In particular, Applicants disagree that Lee discloses, at the very least, the claimed token device that operates to make an integrity challenge to the monitoring component and that will not undertake specific actions of which it is capable unless it receives a satisfactory response to the integrity challenge. The Examiner asserts the Lee discloses this limitation at col. 6, ll. 52-67. The passage cited reads:

> Authenticate Host Routine 310 is provided to allow a card to determine whether the processing

> system in which the card is inserted is authentic. Under routine 310, the card generates a random number and transmits it to processor 122. Processor 122 receives the random number, encrypts the random number based upon an algorithm and an identifying key stored in memory 126, and returns the encrypted random number to the card. The card decrypts the received number from processor 122 based upon the same algorithm and an internal key stored in the card. Again, the internal key uniquely identifies the card as being authentic. The card compares the original random number with the decrypted random number. If they are the same, the card determines that system 100 is authentic. In contrast, if they are different, the card determines that system 100 is not authentic.

Applicants can discern no teaching in this passage nor, for that matter, anywhere else in the disclosure or claims or drawings of Lee that clearly specifies (or even hints at) what happens after the card determines that system 100 is not authentic. Contrary to the Examiner's assertion, Lee does not teach, mention or hint anywhere that the card will not undertake specific actions unless it receives a satisfactory response to an integrity challenge. Lee in fact is concerned with the security of the host computer 100 against malicious code on the smartcard, and teaches only that the host computer and its resident application module may refuse to perform certain actions such as transfer data, etc. (Please see, in particular, discussion at col. 8, ll. 49-67). There is absolutely nothing in Lee that can possibly be understood as teaching that the smartcard may refuse to perform certain actions, under any type of circumstances.

Applicants wish to respectfully remind the Examiner of the requirements posited by MPEP 2143.03 that "[t]o establish *prima facie* obviousness of a claimed invention, all

the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). All words in a claim must be considered in judging the patentability of that claim against the prior art. *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970)." (emphasis added) The Examiner has not made, and indeed cannot make, a *prima facie* showing that the combination of Lee and Strunk is in fact anticipatory of claim 1. Applicants therefore submit that claim 1 is allowable and respectfully request the Examiner to reconsider and pass the claim to issue.

Claims 2-16 depend from claim 1. "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious." *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Therefore, in light of the above discussion of claim 1, Applicants submit that claims 2-16 are also allowable, and these claims are not further individually addressed herein.

With regards to claim 17, the Examiner cites to Lee col. 7, ll. 52-61 as disclosing that the computer platform displays the verification data on a visual display screen. Applicants respectfully disagree. The cited passage teaches that

> Verify Authorization Routine 360 determines whether the user is authorized to use the card inserted into system 100. Under routine 360, system 100 prompts the user to enter a PIN. Processor 122 encrypts the PIN and transmits it to the card. The card decrypts the received PIN and compares it with a PIN stored in the card. If the PINs match, then system 100 determines that the user is authorized and allows the user to gain entry into system 100. However, if the PINs do not match, then system 100 determines that the user is not authorized to use the card.

Applicants discern no teaching in this passage, nor anywhere else in Lee, of the host computer displaying verification data verifying correct operation of the computer

platform, which by the Examiner's reasoning is akin to Lee's random number (see col. 6, ll. 53-65, which is cited to by the Examiner as disclosing the receiving of the response to the integrity challenge, and which discloses the exchange of an encrypted random number, not a PIN). This passages does not address the random number exchanged between the smartcard and the monitoring component, and for that matter also does not teach that the host computer displays the PIN entered by the user. Regardless, the PIN has nothing to do with an integrity challenge from the smartcard to the monitoring device, as per Applicants' claim. Applicants therefore submit that claim 17 is allowable and respectfully request the Examiner to reconsider and pass the claim to issue.

Claim 18 stands rejected "as applied to the like elements of claims 1, 13, 14 and 15 stated above." Because Applicants have addressed the patentability of claims 1, 13, 14 and 15 previously, they now submit that claim 18 is likewise allowable in view of their prior comments.

Claims 19-24 depend from claim 18. Therefore, in light of the above discussion of claim 18, Applicants submit that claims 19-24 are also allowable, and these claims are not further individually addressed herein.

With regard to claim 25, the Examiner finds that Lee does not disclose a monitoring component performing a monitoring operation of a computer platform in response to a received interrogation request signal, nor the monitoring component reporting a result message to said interface, the result message describing a result of the monitoring operation, but that Sprunk discloses these limitations. Applicants have previously traversed the Examiner's combination of these two references as completely devoid of any motivation for the skilled person. Furthermore, Sprunk is directed to members of a network group interrogating one another, and contains absolutely no teaching of a computing entity specifically comprising a monitoring component as claimed. The passages of Sprunk cited to by the Examiner contain nothing but broad descriptions of providing "an opportunity to assess the integrity or trustworthiness of each member" and determining "if the member can successfully complete a secure test operation." There are no specific details disclosed whatsoever regarding such

assessments and tests, and Applicants respectfully submit that the combination of Lee and Sprunk not only is improper due to lack of proper motivation but also falls short of disclosing all claimed limitations, and thus request that claim 25 be allowed.

Claims 26-31 depend from claim 25. Therefore, in light of the above discussion of claim 25, Applicants submit that claims 26-31 are also allowable, and these claims are not further individually addressed herein.

With regards to claim 32, the Examiner asserts, *inter alia*, that Lee discloses that by receipt of a satisfactory result message, the token device offers functionality to the application, at col. 8, ll. 49-57. Applicants respectfully disagree. This passage teaches:

> If verification is successful, application program 400 causes processor 156 to receive debit information from the card, such as an account number, maximum debit per day, maximum debit per transaction, and total debit per day, through CAPI. Under control of program 400, processor 156 communicates with a system belonging to the user's bank (not shown) via serial port 154, or alternatively modem 130, to verify that the user's account contains sufficient funds to cover the charge.

Application program 400 is resident on the application module, and has nothing to do whatsoever with any functionality that may be residing on the smartcard. This entire passage is directed to functions performed by the application module, not the smartcard. Furthermore, as previously explained in great detail, Lee does not address anywhere the concept of the smartcard denying functionality access to the host computer under any type of circumstances. Applicants therefore submit that claim 32 is allowable and respectfully request the Examiner to reconsider and pass the claim to issue.

Claims 33-37 depend from claim 32. Therefore, in light of the above discussion of claim 32, Applicants submit that claims 33-37 are also allowable, and these claims are not further individually addressed herein.

With regards to claim 38, the Examiner cites to Lee col. 6, ll. 37-52 as teaching programming a token device to respond to a received poll signal from an application program, said poll signal received from the computer platform, and the token device receiving a poll signal from the computer platform, and again invokes Sprunk for allegedly teaching the monitoring component performing a verification operation of the computer platform in response to the received signal from the token device. Applicants direct the Examiner's attention to the previous discussion of Sprunk with regard to claim 25, and reaffirm their prior traverse. Furthermore, and contrary to the Examiner's assertion, Lee does not teach the alleged limitations. The cited passage teaches:

> Authenticate Card Routine 300 is provided to allow system 100 to determine whether a card inserted into one of the card units is authentic (e.g., issued by an authorized institution). Under routine 300, processor 122 generates a random number and transmits it to the card. The card receives the random number, encrypts the number based upon an algorithm and an "internal key" stored in the card, and returns the encrypted random number to processor 122. The internal key uniquely identifies the card as being an authentic card. Processor 122 decrypts the number based upon the same algorithm and an identifying key stored in memory 126. Processor 122 compares the original random number and the decrypted random number. If they are the same, processor 122 determines that the card is authentic. In contrast, if they are different,

> processor 122 determines that the card is not authentic.

Contrary to the Examiner's assertion, there is nothing in this passage that teaches the receipt of a poll signal from the host computer. In view of all of the above, Applicants submit that claim 38 is allowable and respectfully request the Examiner to reconsider and pass the claim to issue.

With regards to claim 42, the Examiner cites to Lee col. 7, ll. 17-34 as teaching the token device responding to the poll signal by providing a request for obtaining verification of a state of the computer entity and the token device receiving a result message, the result message describing the result of the verification. Applicants respectfully disagree. The cited passage teaches:

> Authenticate Message Routine 340 allows a card to determine whether data from system 100 is authentic. Secure processor 122 generates a message authentication code (MAC) from data that processor 122 transmitted to the card based upon an algorithm and a MAC key stored in memory 126 and transmits the MAC to the card. The card generates its own MAC from the data it received from processor 122 based upon the same algorithm and a MAC key stored in the card. The card compares the MAC generated by the card and the MAC generated by the processor 122. If they are the same, the card determines that the data is authentic. In contrast, if they are different, the card determines that the data is not authentic. This routine 340 can also operate to allow processor 122 to determine whether data received from a card is authentic. In that case, processor 122 compares the MACs generated by

```
processor 122 and the card and makes a
determination of whether the data from the card
is authentic.
```

This passage thus teaches that the smartcard can verify that data from the host computer is authentic. There is nothing in this passage regarding the receipt of a poll signal, nor anything that could possibly be understood as requesting verification of a *state* of the host computer, which is not the same nor even similar to the described verification of the authenticity of data received from the host computer. Applicants thus submit that claim 42 is allowable and respectfully request the Examiner to reconsider and pass the claim to issue.

With regards to claim 43, Applicants reaffirm their previous traverse of the Examiner's combination of Lee and Sprunk as lacking proper motivation, and further disagree that generating the message authentication code (MAC) of Lee is the same as the claimed monitoring component establishing an identity of itself. The MAC is generated from data that the monitoring component has transmitted to the smartcard (col. 7, l. 19-22) and a key, and has nothing to do with the identity of the monitoring component but rather is directed to the authentication of the data transmitted to the smartcard. Applicants respectfully submit that claim 43 is not in fact anticipated and request the Examiner to reconsider and pass the claim to issue.

With regards to claim 44, Applicants direct the Examiner's attention to the previous discussion regarding claim 1, wherein it is explained in detail that Lee does not in fact disclose the smartcard denying any sort of functionality to the host computer for any reason. Applicants therefore submit that claim 44 is also allowable and respectfully request the Examiner to reconsider and pass the claim to issue.

Claim 41 depends from claim 44, and is therefore also submitted to be allowable.

Claims 45-47 depend from claims that have been previously addressed, and are therefore also submitted to be allowable.

Claim 48 is not specifically addressed by the Examiner, but Applicants note that this claim is similar to claim 1 which has been addressed previously, and thus submit that claim 48 is allowable for the same reasons that claim 1 is allowable.

Claims 49-58 are dependent from claim 48 and therefore are also submitted to be allowable.

With regards to claim 59, Applicants reaffirm their previous traverse of the Examiner's combination of Lee and Sprunk as lacking proper motivation, and thus respectfully submit that claim 59 is not in fact anticipated and request the Examiner to reconsider and pass the claim to issue.

Claims 60-61 are dependent from claim 59 and therefore are also submitted to be allowable.

Applicants acknowledge with gratitude the Examiner's indication of allowability as to claims 6-8 and 35, but as set forth above, believe that all claims are in fact allowable.

Regarding the prior art made of record by the Examiner but not relied upon, Applicants believe that this art does not render the pending claims unpatentable.

In view of the above, Applicants submit that the application is now in condition for allowance and respectfully urge the Examiner to pass this case to issue.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this response is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is being deposited with the United States Post Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

May 25, 2005
(Date of Transmission)

Susan Papp
(Name of Person Transmitting)

Susan Papp
(Signature)

05/25/05
(Date)

Respectfully submitted,

Robert Popa

Robert Popa
Attorney for Applicants
Reg. No. 43,010
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile
rpopa@ladasparry.com